NHS Connecting for Health	**Password Policy for Non-Spine Connected Applications**			
	Programme	NPfIT	**Document Record ID Key**	
	Sub-Prog / Project	Infrastructure Security		
	Prog. Director	Chris Wilber	Status	Approved
	Owner	James Wood	Version	1.0
	Author	Craig Cantwell	Version Date	08/07/10

Password Policy for Non-Spine Connected Applications

Good Practice Guideline

Amendment History:

Version	Date	Amendment History
0.1	01/03/09	First draft for comment.
0.2	01/05/09	Formatting and Additions.
0.3	15/05/09	Formatting and Additions.
0.4	21/05/09	Draft ready for approval.
0.5	28/05/09	Further amendments prior to approval.
0.6	29/05/09	Further amendments prior to approval.
0.7	29/05/09	Minor amendments prior to approval.
0.8	22/07/09	Amendments after comments from Head of IT Security
0.9	08/02/10	Amendments after further comments from Head of IT Security
1.0	08/07/10	Approved

Forecast Changes:

Anticipated Change	When
Annual Review	2011

Reviewers:

This document must be reviewed by the following:

Name	Signature	Title / Responsibility	Date	Version
Infrastructure Security Team		Peer Review		0.1

Approvals:

This document must be approved by the following:

Name	Signature	Title / Responsibility	Date	Version
James Wood		Head of IT Security		1.0

Distribution:

NHS Connecting for Health Infrastructure Security Team Website

http://nww.connectingforhealth.nhs.uk/infrasec/gpg

Document Status:

This is a controlled document.

Whilst this document may be printed, the electronic version maintained in FileCM is the controlled copy. Any printed copies of the document are not controlled.

Related Documents:

These documents will provide additional information.

Ref no	Doc Reference Number	Title	Version
1	NPFIT-SHR-QMS-PRP-0015	Glossary of Terms Consolidated.doc	13
2	NPFIT-FNT-TO-INFR-SEC-0001	Glossary of Security Terms	Latest

Glossary of Terms:

List any new terms created in this document. Mail the NPO Quality Manager to have these included in the master glossary above [1].

Term	Acronym	Definition

Contents

1 About this Document

1.1 Purpose

The purpose of this document is to provide guidance to NHS organisations on the various aspects of Password Management. This will include the use of passwords to control access to data, how to manage passwords effectively and good practices around password use within the NHS.

This document should be used as guidance when setting policies for password management for organisations, and when implementing new systems that require secure authentication[1] controls.

After reading this document the reader should understand:

- Good practice guidelines regarding secure use and handling of passwords.
- The different ways to manage passwords within an organisation.
- Password formats.
- Security risks associated with poor password management.

1.2 Audience

This document has been written for readers who have a responsibility for IT Security Support within an area, Systems Administrators, Policy Makers, contractors and third parties where relevant and other interested parties within the NHS.

1.3 Content

This document comprises this following sections / topics

- Introduction.
- Secure use of Passwords.
- Setting password policy.
- Password Management.
- Risks and Mitigation.

1.4 Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement,

[1] Authentication – The process during which a user proves that they are a particular legitimate user by providing the answer to a question, username and password etc.

recommendation, or favouring by NHS Connecting for Health. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

Any party relying on or using any information contained in this document and/or relying on or using any system implemented based upon information contained in this document should do so only after performing a risk assessment. It is important to note that a risk assessment is a prerequisite for the design of effective security countermeasures. A correctly completed risk assessment enables an NHS organisation to demonstrate that a methodical process has been undertaken which can adequately describe the rationale behind any decisions made. Risk assessments should include the potential impact to live services of implementing changes.

This means that changes implemented following this guidance are done so at the implementers' risk. Misuse or inappropriate use of this information can only be the responsibility of the implementer.

2 Introduction

This document discusses the issues associated with the use of passwords and the management of passwords. These will include:

- The benefits and limitations of different password formats.
- An overview of the way passwords can be used and stored.
- Guidance on system design regarding password use.
- The balance between security and usability.
- Examples of ways passwords can be compromised and how to defend against attacks.

2.1 Background

Authentication is the process by which a system or data store verifies that the identity presented by a user pertains to that user. This is done using an "authentication factor"- a piece of information used to authenticate or verify a person or application for security purposes. Authentication factors can take a variety of forms, from the traditional user name and password, to tokens or biometrics. Generally authentication factors fall into one of the following 3 categories:

- Something you have (e.g. tokens).
- Something you know (e.g. password/passphrase).
- Something you are (e.g. biometric – fingerprint, iris scan).

A potential fourth factor/option could be 'Somewhere you are' this could be logging onto a system from a particular terminal or location. Location could be determined the IP address or subnet of the source (IP addresses may be able to be faked or 'spoofed' unless adequate protection is taken). This potential fourth factor may be more of an authorisation factor rather than authentication

Once a user has been authenticated to a system, authorisation (defined in this context as a set of permissions that can be applied to a user) functions can then be used to restrict or grant access to certain functions, services, files, and servers.

It should be understood that authentication is a separate concept to authorisation. Authentication is a process of identifying a user based on their credentials (typically username and password), whereas authorisation is a process of determining whether an authenticated user is allowed access to a specific resource or not. The NHS CRS Smartcards[2] are an example of a type of authorisation.

Due to the importance, sensitivity and value of the information being stored on NHS systems, effective authentication of users is an essential part of the security of an

[2] NHS CRS Smartcards - http://www.connectingforhealth.nhs.uk/systemsandservices/rasmartcards

NHS organisation's IT (Personal Identifiable Data must be protected to eGIF[3] level 3). As such, appropriate controls, policies and procedures in relation to passwords should be implemented.

Passwords were the first logical authentication mechanism used to protect computer systems and are still the most widely used.

As such, the creation of a password policy and appropriate procedures will ensure that minimum standards can be set and adhered to by an organisation.

[3] e-Government Interoperability Framework Version 6.1 - http://www.cabinetoffice.gov.uk/govtalk/policydocuments/e-gif.aspx

3 Secure use of passwords

Passwords and Personal Identification Numbers (PINs[4]) are used extensively within both workplace and retail environments to authenticate to information systems and financial resources. This extends to online shopping/ bank accounts, email services and Patient Administration Systems, as each of these use passwords to provide an elementary level of access control.

Due to the wide usage of passwords within both the workplace and domestic contexts, keeping track of passwords becomes increasingly difficult, additionally, when updating passwords it is often difficult to choose passwords which are of sufficient complexity yet still easy to remember. With this in mind, secure and repeatable methods for managing passwords are recommended to ensure a high standard of authentication to critical information resources within an NHS organisation, as the information held within NHS information resources includes Patient Identifiable Data, and as such requires strong methods and policies to maintain the integrity, confidentiality and availability of this data. This need is reinforced by NHS organisations legal requirement to adhere to the Data Protection Act.[5]

3.1 Using passwords securely

Many people use passwords in an insecure way and this is done for a number of reasons. (Some of the reasons may be considered valid within an organisation and will likely identify areas where policy and/or procedures may need to be changed - see the section on Password Policy). Because of this, the following should be considered:

- Password Protection.
- Password sharing.
- Multiple passwords.
- Password storage.
- How to choose good passwords.

3.1.1 Password Protection

The following list contains a number of simple techniques that can assist in the protection of a password:

- When entering a password, ensure that no-one is able to see what is being typed in.

[4] PIN – This is normally a short password often 4 digits long. Containing only numerical characters (0-9).

[5] See Data Protection Act - http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

- "Shoulder surfing" is a common way for thieves to see a PIN while it was entered in a shop or into an ATM (cash machine). This is relevant to the NHS when considering where PINs and passwords are used (e.g. authenticating with the NHS Smartcard & gaining access to restricted areas), and as such, users should attempt to ensure that the entry of their PIN or password is suitably hidden from view - example by using their other hand to cover the keystrokes
- Mobile phones are not seen as a secure place to store passwords & account information (they are easily stolen, most are not encrypted and do not have a PIN set). If a potential attacker sees someone using their mobile phone to lookup user account information then they are likely to be a target.
- Diaries and notepads are also not seen as a secure place to store passwords for similar reasons to mobile phones. If a potential attacker sees someone using their diary to lookup user account information then they are also likely to be targeted.

There are very simple user actions which can be used to secure passwords in daily use, effective training and awareness is a good way of implementing this.

3.1.2 Password sharing

Password sharing, defined in this context as a single user account used by more than one person, can create a number of issues when considering the integrity and availability of data. One of the issues caused by users not having individual credentials is that audit can be compromised- i.e. if the user recorded against a transaction (for example the update of the allergies field in a person's medical record) is not stated as a specific individual, then exactly who made the transaction cannot be determined. This is important when considering legal challenges to data records- i.e. in the instance of potential legal proceedings.

There may be genuine reasons why password sharing is needed, however a lot of the reasons may only be for convenience and not be valid reasons. It is not recommended to share passwords. Some NHS organisations may have polices on password/account sharing as they may allow it for operational reasons; however this is not consider good practice and exceptions to this should be carefully considered and assessed.

Some of the reasons why passwords are shared are:

- Shared workstations (shared workstations doesn't have to mean that passwords are shared although they often are)
- Generic accounts (e.g. Administrator and Root accounts)
- Speed of access
- Lack of policy
- Lack of knowledge
- Culture

- Convenience

Password sharing can also cause the following issues:

- Shared passwords are more likely to be written down or known by those who do not need to know them.
- Accounts are more likely to be locked. One of the valid users may be prompted to change the password however a different valid user may attempt to access this account before the first user has notified the other users of the shared username and password making a number of attempts and locking the account. This in turn causes more calls to the helpdesk for accounts to be unlocked.
- This also may lead to the use of sequences of passwords in order to avoid the account being locked. (e.g. Password1, Password2, Password3 etc) Therefore after a number of attempts the user tries the next iteration of the password hoping that a previous user had changed the password.
- Users may have to manage the distribution of the shared passwords with all other users of the same account and password. This creates additional management overhead for the user.
- Weak passwords are more likely to be used so that more than one person can remember the password.

Based on the above, it is recommended that users should only have access to the applications necessary for them to perform their duties. If there is a need for someone to access something that is normally inaccessible by them then a request should be made and approval given by the appropriate person.[6]

Password sharing significantly increases the risk of systems being compromised.

3.1.3 Multiple Passwords

Users should set distinct passwords for each system they access. However due to the potentially great number of systems a user may have access to, many passwords have to be remembered, as such there is a temptation is to set all these passwords to be the same. This reduces the number of unique passwords a user has to remember, however as these are not likely to be linked in terms of their expiry timings, confusion and administrative overhead can increase significantly. Additionally, if the user's password is compromised for any reason, all the systems that user had access to will be vulnerable.

Another factor in this area is that users may be tempted to use the same passwords for highly sensitive systems and relatively insecure systems. Even if strong passwords are used they may still be compromised if used to access the wrong web site or on-line account. Strong passwords are more difficult to crack a typical strong

[6] More information on this and other security principles are available in the General principles for Securing Information Systems Good Practice Guideline - http://nww.connectingforhealth.nhs.uk/infrasec/gpg

password will have a combination of the following: Uppercase, Lowercase, Numeric & Non alphanumeric characters. The password should not contain all or part of the username or personal information. A minimum length should be set of at least 8 characters.

With this in mind, enforcement of organisational policy can become more difficult as it is extremely challenging to tell if the user has used the same password across multiple accounts. Solutions like Single Sign-On (SSO) can remove the need to remember passwords for multiple accounts (see section 4.4 'Synchronisation of passwords and Single Sign On')

3.1.4 Password Storage

A consideration for organisations implementing password policies that require a greater volume of passwords, and for those passwords to be more complex (and as a result more difficult to remember) should be the use of password storage and management solutions. An appropriately considered and procured solution can mitigate many risks, some of which include users writing down their passwords on post-it notes or within notepads, or even within simple spreadsheets on their own PCs. Some examples of password storage are:

- Physical methods (such as locking important account credentials in a safe for disaster recovery purposes).
- Hardware/software methods such as bespoke appliances an application running on a PC or server.

The section on Password Management below provides additional information on such technologies.

3.1.5 How to choose strong passwords.

The "strength" of a password is defined as how difficult it is to obtain without prior knowledge of it. This can take the form of guessing the password, or employing "brute force" password guessing software. In this latter instance, the strength of a password can be stated as how long it would take to "brute force" it. In order to provide greater levels of security, strong passwords should be chosen by users.

Some helpful tips are shown below:

- Mix letters, numbers and symbols, and use case sensitivity (upper and lower case letters). This mixture is known as "pseudo-random alpha-numeric combination"; using this, it is almost impossible to "crack" somebody's password (i.e. instead of "password," try "pAsS34%(6*2woRd," etc.).
- Find a good way to remember the password. A good way to do this is to choose the first letters of a sentence that will be memorable. e.g. *"I own 2 rabbits called Thumper and Bugs"* gives: Io2rcTaB
- Use punctuation to aid complexity. To incorporate a colon into the previous example, remember the sentence as *"I own 2 rabbits: Thumper and Bugs"*, which would give: Io2r:TaB
- The longer the better. A recommended minimum for a password is 8 characters, however this should be subject to organisational policy shorter passwords can be more easily deduced from a brute force attack.

- One other way is to use a word, for example, healthcare, and move up one row on the keyboard. Healthcare becomes y3qo5tdq43. (add in capital letters for increased complexity)
- If possible, try to use "nonsense words." Combine these with numbers and/or punctuation to make memorable, secure passwords. For example, "glassphone3895."

This list is not exhaustive, and users are likely to use methods that appeal to them personally.

Additionally however, the below lists some common pitfalls that should be considered:

- Users should not tell anybody their passwords. Somebody could overhear it or the person told could let it slip.
- Users should not use any passwords within this document (or indeed any similar documents); they are now openly known and easy to find.
- Users should not write their passwords anywhere where it might be seen or found.
- Users should not tell anyone the method that has been used for the creation of passwords.
- Users should not base their passwords on well known information about themselves.

3.2 General security and awareness

Security measures/passwords should not be a hindrance to daily duties; instead they should be seen as an important part of the system/s they are protecting. It is recommended that users should be educated so that they understand the importance of their passwords, and understand how important they are to the security of systems.

There is a great amount of emphasis and reliance on users regarding password security as the biggest vulnerability lies with the user. A combination of securing systems and educating users backed up by a good password policy is crucial to minimising the risks.

4 Setting Password Policy

A fundamental part of password management on an organisational level, is the Password Policy[7]. This policy will serve to set the standards to which all systems in use within the organisation should adhere in terms of their password use. Additionally, an organisation's security policy should include all aspects of password assurance, and address the following questions:

- How long should a password be and how complex should passwords be?
- How does a user request a password?
- How are requests for access (e.g. a new starter requiring access to systems/services or someone who has had a change of role) dealt with?
- What happens in the event that unauthorised access is detected?
- What is the process for instigating disciplinary action against someone for not complying with the policy?
- How often will the policy be reviewed?

The following section will go into a number of the areas that may be defined within a password policy.

4.1 Password Strength

The 'stronger' the password, the less likely it is to be compromised. The factors that define the "strength" of a password include the following:

- Complexity: The more complex a password is made then the greater the entropy of the password becomes. Entropy is a measure of the uncertainty of an outcome, in the case of passwords the greater the number of differing factors used to create the password (length, characters used) the lower the chance of the password being guessed or derived by brute force methods.
- Length: the length of the password is relative to its strength. Shorter passwords will be compromised more quickly via brute force attacks as there are fewer combinations of characters possible within the password.

The complexity of the password must also be considered. In general, passwords can be constructed by allowing characters from any combination of the following four character groups:

- Lower case letters
- Upper case letters
- Numbers
- Non-alphabetic characters (such as !, ?, £ etc.)

[7] As with all policies HR should have some involvement in this process. They are responsible for enforcing any disciplinary action as required.

Some applications and systems can enforce password complexity (such as Microsoft Windows) and it is considered good practice to use passwords which contain characters from three of the four character groups.

In addition, further complexity requirements can often be enforced, such as not allowing consecutive characters in a password to be the same, not allowing parts of the username or user ID to be included in the password and so forth.

To avoid the situation where passwords are written down as an 'aide memoir' due to complexity, it should be ensured that password rules keep the password as practical and useable as possible. A balance must be achieved between complexity and usability. It is for this reason that many organisations choose to use 'passphrases' over 'passwords'.

It is recommended that passwords used meet these minimum standards:

- Passwords should not contain all or part of the user's account name.
- Passwords should be at least 8 characters long.
- The previous 4 passwords should not be used.
- Passwords should contain characters from three of the following four categories.
    - Uppercase characters (A…Z)
    - Lowercase characters (a…z)
    - Base 10 digits (0…9)
    - Non alphanumeric (such as !, ?, £ etc.)

Care should still be taken to ensure passwords are strong, as "Password1" and "Passw0rd" etc may fit into the allowed complexity and length however they are still very weak (this is very difficult to enforce, and so user education in the importance of strong password use is key in this area)

4.2 Passwords or Passphrases

Passphrases[8] generally differ from Passwords in a number of ways. One way is length with a password typically 6 to 10 characters long and a passphrase being much longer, often 20 to 30 characters. Passphrases can be easier to remember - consider the passphrase: "My favourite food is pizza" compared to a complex password of "5Ftgd7(!". Due to their increased length, passphrases are less susceptible to brute force attacks.

Care should be taken not to choose a phrase direct from a phrase or quote dictionary as the risk of a successful dictionary attack will be increased. If applications or systems allow the use of spaces in password/passphrases, then this can also help the users remember the phrase and adds another character into the complexity of

[8] A passphrase is a series of words (may not be meaningful) easily remembered by the user.

the passphrase (this is an easy way to increase complexity but in general the need for complexity can be lessened due to increased length of the passphrase).

Generally passphrases are regarded as more secure than typical passwords. However, this does not mean that every system/application should use passphrases as it is much harder to ensure that the user chooses a passphrase that meets standards set to avoid dictionary attacks. Some older systems may not support passwords/phrases over certain lengths and are not able to use passphrases and a good/strong password should be used instead. This is typical of Windows systems using NTLMv1 as passwords of over 7 characters long are separated into 7 character sections before hashing this means that when attempting to crack a password it can be done in 7 character chunks and re assembled, also in an NTLMv2 environment if passwords of longer than 14 characters are used then this will not be compatible with NTLMv1 systems.

4.3 Password Expiry

All passwords should have an expiry date/time[9], therefore a policy stating that passwords should be changed every X days and applications & servers setup to support this is recommended.

The more complex a password (the greater the entropy of a password) then the less often it will require changing to maintain a good level of security. Generally good practice would suggest that passwords should expire after 30-90 days (depending on the type of account, administrator passwords should generally be changed more frequently than regular users passwords), and it is also considered good practice to ensure that when a password is changed, one of the previous passwords should not be used- this is often be set to the last 4-12 passwords (which typically mean that the user should not be able to use any of the passwords used previously for a time period of 1 year or more). The password policy should reflect this and systems should be configured to not allow passwords that contravene the policy.

It is recommended that accounts are disabled that have either not been in use for a protracted period, or are otherwise not required, as dormant accounts can be exploited- for example, where staff have changed roles or have been given unnecessary access to a system/application, and the account used is therefore no longer required.

If a user requires their account to be unlocked, then they should follow a similar procedure for someone that has forgotten their password. See Account Creation & Resetting Passwords.[10]

[9] Every time a password is changed then a brute force or dictionary attack will have to be restarted to ensure success.

[10] Please also see other GPGs that refer to access control and authorisation. http://nww.connectingforhealth.nhs.uk/infrasec/gpg

4.4 Synchronisation of passwords and single sign on

Password synchronisation[11] and Single Sign-On (SSO)[12] are both types of identity management software solutions. Password synchronisation is often considered as being less resource intensive to implement than SSO as there is no client software deployment. Password Synchronisation is also seen as less secure than SSO as generally there is only one password to get into many systems, where as with SSO the password is often combined with another factor of authentication to provide 2-factor authentication[13].

Most enterprise SSO solutions will automatically manage the backend password enabling the password to be set to the maximum length and complexity possible for the system as these passwords are never known to the users this in turn will make the individual systems more secure.

Some of the advantages of these solutions are:

- Users with SSO or Synchronised passwords are more likely to remember them.
- Less password related calls to the service desk (can help reduce some operational IT costs or free up staff to provide a better level of service).
- System can provide reporting (can be useful for compliance as detailed reports may be produced giving information on account activity).
- The fewer passwords a user has the less likely they are to write them down.
- Users may be more willing to have a stronger password if they have less to remember.
- Increased productivity due to the need to enter only one password instead of several.

Some of the disadvantages of these are:

- If compromised then access is gained to not just one system but several.
- Can be very difficult to implement in environments with a large number of systems on different platforms and if using bespoke software.

When setting the requirements for such a solution, the following factors should be considered:

- Availability (is the solution required 24x7? How long could the organisation tolerate access to the solution being unavailable?).

[11] Password synchronisation – A process or technology that helps users maintain a single password across multiple systems. On accessing each system then the user will have to authenticate unlike in Single Sign On.

[12] Single Sign On - A user/session authentication process permitting users to access multiple data sources after providing authentication credentials once. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session. Part of an integrated access management framework.

[13] Two factor authentication – Authentication based on two factors (usually a password and something else like a token or biometric)

- Backup capabilities.
- Scalability.

Any system should be developed and configured to support organisational password policies, any procurement should be aligned to strategic/policy goals. As with any solution there should be an effective audit function with adequate resource to review reports.

4.5 Account creation & Resetting passwords

A key element of password management is the creation and maintenance of a process to create accounts & passwords. Ideally this will involve the organisation's HR function so as to ensure that new starters, staff moving within the organisation, and leavers will be processed swiftly. This in turn would reduce the risks associated with new users having to make use of accounts not attributed to them until such time as their access can be properly granted.

Additionally, periodical reports (daily, weekly or monthly) should come from HR detailing changes to personnel so that the systems can be kept as secure as possible by limiting access only to those that need access to perform their roles.

Once an account has been created, details of this account and password should be treated securely (for example a username should not be sent in the same message as a password especially if that message is in clear text). Often the username is sent out on an email and the password will be given over the phone in person at a user's induction or when the users IT equipment is handed over to them.

If a user has forgotten their password or their account has been locked out, then the user should contact the team responsible for resetting passwords and request that this is done (account reset queries should only be made by the person who the account belongs to). Checks should be made to verify that the user is who they say they are and then the account can be unlocked or the password reset. Again the password should not be sent out in a message in clear text, it should be treated in a secure manner.

All systems and applications (where possible) should be setup so that users will be forced to change their password at first time of logon after the creation of a new account or a password reset.

4.6 Generic passwords/accounts

Where possible the use of generic passwords should not be permitted within the organisation's password policy, however there may be certain circumstances where a generic password is unavoidable (root & administrator passwords for example). It is generally considered good practice to segregate privileged account usage and provide access to privileged systems and functions through a federated authentication model where possible.

These accounts should be subject to stricter password expiry rules, however a procedure must be in place so that when passwords are changed, users of these accounts are made aware (in a secure manner) and the old password is not entered, potentially locking the account. It is recommended that a procedure is put in place to change all privileged passwords if one of the administrators leaves the organisation.

Generic passwords generally mean that a number of people will all have access to the one account using the same credentials. This means that audit and accountability for a user's actions should be maintained via alternative means. As this is a potentially resource intensive process, it highlights the need for the use of generic credentials to be in as minimal a use as possible. This is due to the risk of if there is a breach there may be no way of telling where it came from and if an amendment is made to a data record again there may be no way of knowing who made the change. Within the context of the NHS, audit and accountability of changes to patient records is critical.

4.7 Enforcing Password Policy

The enforcement of the password policy has two key focuses, one on the users of the systems (who hold the passwords) and secondly on the systems and applications themselves. In order for a policy to be enforceable the policy must be created in collaboration with all key stakeholders to ensure the policy is of an acceptable standard.

4.7.1 Users

Users are the holders of the passwords and as such they are a focal point to ensuring the security of the systems.

- Training all staff on secure use of passwords (preferably as part of a general Information security training exercise) and afterwards getting them to sign off that they have attended the training, understand it and agree to the policy.
- Performing audits or random checks on the users to ensure that they are complying with policy (not hiding passwords under keyboards etc.).
- It may be necessary to take action when a blatant disregard for the policy has taken place and risks to patient care/confidentiality have been severely increased. If this is the case then the HR Department and the users Manager will need to be involved. This is an important reason why it is good practice to ensure the involvement of HR when setting the policy as they will understand and will be able to give advice about employee's rights and employment law.
- One way of ensuring that users keep their passwords secure is by making personal information accessible to the account holder (when the security of someone's personal information or belongings is at risk then the user is more likely to take precautions to reduce the risk). This is often seen as a last resort as the first three points should be considered before considering using personal information.

4.7.2 Systems

The recommended way to enforce a password policy is by having systems & applications setup to support this (where possible). This can be done in a number of ways including:

- Ensure that applications and systems are setup to only allow passwords meeting the minimum level of complexity and length.
- If possible applications/systems should generate the initial password for user and send in a secure manner.
- When new users are created, make sure that the password must be changed at time of first logon.
- Ensure that applications/systems will lock accounts after x number of failed attempts to login (if possible to enforce due to healthcare constraints).

In addition the performance of regular security testing can assist in ensuring systems and applications are configured in a manner that supports the password policy. Regular audits should be performed to make sure systems are configured correctly and that any issues highlighted during testing have been resolved.

5 Password Management

Passwords can be managed in a number of ways, from appropriately secured physical lists of usernames and passwords, to complex solutions on hardened servers[14], with both of these being appropriate in certain circumstances. With this in mind, it should be noted that password management processes should be appropriate to the sensitivity of the passwords, systems and services being protected. As such, it is recommended to perform a risk assessment to determine from the organisations perspective what an adequate solution would be for managing passwords with regards to the criticality and sensitivity of the systems being accessed. However, a key point of note would be that appropriate backups for the password management systems should be considered, with appropriate controls placed around the backups.

5.1 Password Management solutions

There is a great variety of password management solutions available from simple password management for personal password to large scale systems interacting with other applications and systems to manage passwords.

5.1.1 Simple password management

Examples of simple password management:

- Spreadsheet containing details of usernames, passwords, systems, URLs etc. This spreadsheet may be stored on a network drive and password protected, however the file is vulnerable to being compromised by a malicious user. Additional measures to protect the spreadsheet are available, however as these are applied in increasing measures, they will be begin to overlap a dedicated password management solution in terms of management overhead and costs. This is not recommended for storage of large numbers of usernames and passwords.

- Hand written or printed list of usernames & passwords. This is one of the least secure methods of password storage. Even if the list is kept in a safe it is still at risk of being misplaced or stolen when being used. Like spreadsheets, the information may be out of date very quickly and will require updating every time a password is changed.

- Stand alone application (software based application that sits on users PC or Laptop). Users are still required to keep passwords up to date by editing objects in the database, however this file is usually encrypted and can be stored in a different location form the application as long as the application points to the file and has read/write access to it.

[14] See GPG on system hardening for more information

There are other simple ways to manage passwords, and the selection above is only given as an example. The main disadvantage of using simple password management is the way that passwords have to be changed manually to match the passwords in the systems. There are also issues when trying to manage administrator accounts using these methods, as numerous people may require access to individual accounts and there may be issues if password management is already in use by someone but also required by someone else.

These simple solutions are not suitable for the management of passwords in all situations, therefore a risk assessment will identify how important the passwords and systems are to the organisations. If the passwords are so sensitive it should be a consideration to use additional measures of protection, an appropriate software or hardware based Password Management solution may be a better option.

5.1.2 Password Management systems

There are a range of different password management systems providing a range of different features. Password Management systems can simply store all passwords in a secure repository or can be completely interactive with the rest of the infrastructure controlling all access and changing passwords.

An example of some of the different types is shown below:

- Software based, installed on a server with client installs required so that users can access password database. Can be integrated with Active Directory or other directories so users can log in with same credentials as PC/Laptop.
- As above, but no client install required users logon to system direct through a web page.
- Software or Hardware Appliance (generally Linux or hardened Windows server), can be configured to monitor and control the access for all users. Can work interactively with applications and systems to ensure that passwords are not out of date and some systems have the ability to change passwords periodically in line with password policy.

Most password management systems can now be configured to work with Active Directory or Novell eDirectory. Depending on the solution chosen some of these systems can require considerable resource to install and configure to utilise the functionality completely however with some the day to day management of passwords is automated.

Password management systems can also be used as a defence against phishing[15] as they are not susceptible to “lookalike” websites or other visual imitations. However they may not be able to automatically handle complex login procedures (for example, if obscured passwords[16] are used see next section on Factor Strengthening).

[15] Phishing – The process of attempting to gain sensitive information such by masquerading as a trustworthy entity (social engineering)

[16] Obscured Passwords – Designed as a way to conceal the entry of passwords from malware by changing the way that passwords are entered into the system.

There are some vulnerabilities associated with password management systems. If the master account is compromised then this renders all passwords contained in the system vulnerable. Some systems will hold an unencrypted copy of the password in memory while it is being used. All proposed solutions should be procured in the usual manner for the organisation and this process should evaluate the product from a security perspective.

5.1.3 Factor Strengthening

One way make it difficult to gain access to a system even if the password has been guessed is by using quite simple grids which means that the user never types in the actual password just a code that represents the password the figure below shows a simple example.

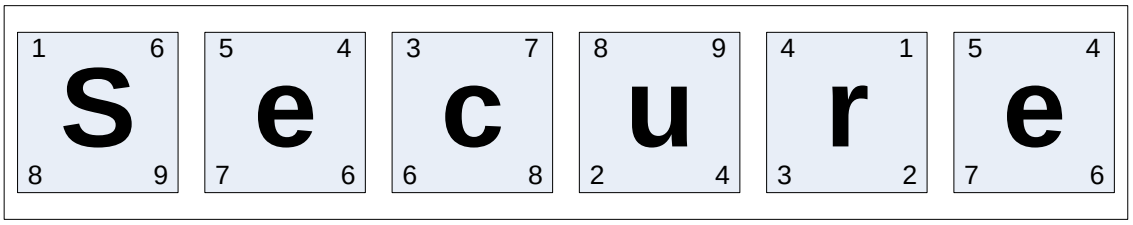

Figure 1

In figure 1 the password is Secure however the letters in the grid are represented as shown and in order to authenticate a user may always choose the top right corner therefore they type in 647914 each time they have to authenticate the grid should change so that the users are not always typing in the same representation of the password. Another way is for the system to prompt the user which corner to use both the grid and the corner can change each time. This is a useful way to make shoulder surfing less of an issue also the risk from key loggers is reduced. Another way which does not use passwords at all uses a defined pattern instead (user could pick lots of individual squares of the grid but generally a pattern will be more memorable). In figure 2 an example is shown where the user would type in 97597514 again each time the user attempts to authenticate the grid will change.

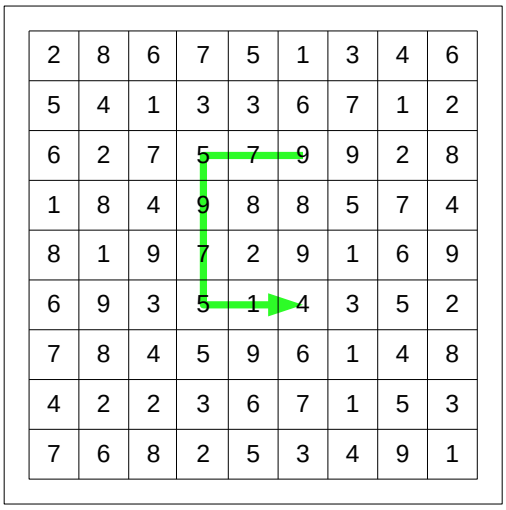

Figure 2

There are a number of other different variations of these types of solutions available, whatever solution is chosen it should be implemented in a secure manner as it may be possible to make the solution easy to crack by choosing small grids and less numbers or characters available in the grid

6 Risks and Mitigation

As with many areas of IT Security, the identification and mitigation of risk is an important step towards ensuring that security controls are well implemented and appropriate.

The following sections detail some of the more prevalent risks associated with the use of passwords, and some of the steps that can be taken to mitigate them.

6.1 Risks/Attack Vectors

The main risks linked to password security can be exploited in a number of different ways some of the main risks are:

- Theft (financial, data or Identity).
- Service Interruption (System malfunction, system overload or Damage/Loss of system).
- Internal risks (Privilege escalation, Fraud, Unauthorised software or inappropriate contents).
- External risks (Hacking, Spoofing user IDs, Social Engineering, Malicious Code Distribution or Undetected Access).

The various attack vectors used to exploit these risks can be grouped together into one of the four following categories:

- Dictionary/Word-list.
- Brute Force/Exhaustion.
- Naivety.
- Discipline.

The list above only represents the most common risks and attacks used, and there are other potential ways and some attacks may use a combination of the above. Attacks can be manual or automated (machine-based). Automated attacks use a computer or number of computers to attempt to ‘guess’ passwords used on a system or within a service. This requires some degree of penetration of the target network/system in order to obtain the password hash[17] file/data for the identified system or service. Manual attacks come via the keyboard only.

[17] Hashing – The one way transformation of a bit pattern to produce a signature (hash). Any change in the original pattern will produce a different signature. Given the hash it should not be practical to find the original bit pattern within a given time.

This section of the document discusses the various types of attack in more detail and will also give a brief explanation of how to protect or defend against them.

6.1.1 Dictionary Attack

Normally, a machine-based attack uses hash values already gathered. This information is then used offline, working through a dictionary/word-list of password possibilities, hashing all of the words in the dictionary/word-list in turn and checking for a match with the hash values previously gathered. A program will normally carry out this function methodically working through likely passwords until the hash of the candidate password matches the hash previously gathered (This process is called 'password cracking').

There are a number of ways in which dictionary attacks can be carried out with a variety of software available commercially and for free (Free password cracking software tools include 'John the Ripper', 'L0phtcrack' or 'Cain and Abel'). The use of 'rainbow tables'[18] makes password cracking quicker and can sometimes make attacks against hashed passwords feasible. To prevent the use of rainbow tables salting[19] can be implemented.

Protecting against dictionary attacks can be done in a number of ways including not allowing user-generated passwords[20] and where this is not possible or practical (which is often the case as people often struggle with passwords they have not selected themselves) enforcing password policy including password complexity rules. Meeting complexity rules does not always safeguard against attack as "Passw0rd" is easily guessable but will meet most complexity rules.

6.1.2 Brute Force Attack

Also known as the 'exhaustion attack', this is another machine-based attack and requires that the attacker has already obtained some password hash values. This can be a slow process (depending on the complexity of the password and speed of the computer or computers being used to run the software) as it will methodically work through all possible passwords again hashing each one and comparing it to the previously gathered hash (cracking). If the password contains 3 letters the attacker will work through all possibilities: aaa, aab, aac……zzx, zzy, zzz (the passwords may not be attempted in this order).

Protection against Exhaustion Attacks differs from dictionary attacks although making passwords complex will help and will also slow the attackers down. An exhaustion attack will always eventually successfully find the password. Therefore, the best way

[18] Rainbow Table – A lookup table used for reference when cracking passwords.

[19] Salt & Salting – The salt is a number unique to a password change interval and a user, every time the password changes so does the salt. This number often contains the users ID or the time. Salting is combining the salt to the password to the password prior to hashing to mean that every time the password changed a brute force attack may have to be halted and restarted.

[20] User generated password – This is a password that the user has come up with. Sometimes this can contain personal information even though the user may have tried not to do so (often sub-consciously a user will relate the password to something so that they can remember it).

to protect from these attacks is by making the time it takes for success to be so long that any potential attacker will deem it not worthwhile.

Length of the password	Character set			
	lowercase letters	lowercase letters and digits	Both lowercase and uppercase letters	all printable ASCII characters
< = 4	instant			2 min
5	instant	2 min	12 min	4 hours
6	10 min	72 min	10 hours	18 days
7	4 hours	43 hours	23 days	4 years
8	4 days	65 days	3 years	463 years
9	4 months	6 years	178 years	44530 years

Table showing how long it takes to Brute Force passwords of differing strengths.[21]

To achieve this, salting can be performed. This will complicate the hash and an exhaustion attack will have to search over a new password space[22] every time the password is changed. Another way is to use a slow hashing process, which will increase the time it takes to process the password once it has been entered. Attacks which rely on making multiple attempts at guessing passwords would result in increasing the time it takes to successfully perform the attack to a level that is not acceptable to the attacker (making sure that the user experience is still at a tolerable level)

Account lockout (after a number of attempts) is also an option. However in certain areas of the NHS it may be deemed to be counterproductive to do this especially if it relates directly to the provision of Healthcare.

6.1.3 Naivety Attack

This attack can be either manual or machine-based and attempts to exploit the failing of users to generate strong passwords. Passwords are often easily guessable or simple/non-complex and sometimes match the username or are similar to the username. Keeping default usernames and passwords is also a common weakness. It is likely that default usernames/passwords will be attempted first by an attacker before any others are tried and indeed, it is possible to obtain lists of manufacturers/vendors default accounts/passwords via the Internet[23]. Attackers will additionally try variations on more frequently used passwords.

A number of ‘password auditing’/’password cracking’ tools exist that will automatically work through lists of commonly used passwords as well as variations of such passwords (such as appending numbers to the end of passwords – e.g. password1)

[21] Calculations based on a single computer with a brute force speed of over 5,000,000 passwords per second. Information in table taken from http://www.lastbit.com

[22] Password space – Either the set of all the possible passwords in a given implementation or the size of the set.

[23] An example: http://www.phenoelit-us.org/dpl/dpl.html

The more personal information the attacker knows about the person whose account they are trying to break into, the more likely it is that the attacker will find out the password of the persons account. This is because often, users will pick passwords that contain a piece of personal information (e.g. pet's names, children's names, holiday destinations and memorable dates are all good examples). Social engineering is one of the ways that an attacker can get hold of personal information that may be used in user's passwords, social engineering can take place a large number of ways from simple conversations to social networking sites and attackers will go through refuse if they believe that the rewards are great enough.

Protecting against naivety attacks can be done in a number of ways including not allowing user-generated passwords (as computer-generated[24] passwords will often be more complex and less likely to use personal information although they are not always easy to remember) and where this is not possible or practical enforcing password complexity rules. Passwords however still have to be usable and memorable so over complicating passwords will result in making the system more vulnerable to 'Discipline Attacks' (also see section 4.1 'Password Strength').

6.1.4 Discipline Attack

This attack is usually a manual attack where the attacker attempts to exploit the user's lack of discipline regarding the storage and/or use of passwords. Passwords may be written down or printed out and stored in an insecure way. A key logger[25] may be installed and running on the user's computer (without the knowledge of the user). A user may be unaware that they are being watched whilst typing in their username and password. The observer may be there in person or even watching the user using a hidden camera, mobile camera phone (the attacker may pretend to be on the phone but are actually recording what is happening). In some instances where users have to remember a large number of different usernames and passwords, the passwords they use may be stored on the computers desktop or network drive in the form of a spreadsheet, word document or text file (often without any protection).

The best countermeasures against discipline attacks are education and training. The greater the awareness on information security and the possible consequences of not securing data the users have, the more likely they are to treat the information securely.

The use of password management solutions can be used to securely store password lists (see section 5 'Password Management')

[24] Computer generated password – Also called randomly-generated. Can create a Strong password however a balance must be achieved between security and usability. Having randomly generated passwords of 20 characters long may be overkill and may result in insecure password management by users in order to remember their passwords.

[25] Key Logger – Can be hardware or software which capture and record user's keystrokes.